

REMARKS

The application has been reviewed in light of the Office Action dated November 10, 2004. Claims 1-19 are pending in this application, with claims 1 and 8-11 being in independent form. It is submitted that no new matter has been added and no new issues have been raised by the present Amendment.

Claims 1-19 were rejected under 35 U.S.C. §102(b), as allegedly anticipated by U.S. Patent No. 5,826,013 to Nachenberg. Applicants have carefully considered the Examiner's comments and the cited art, and respectfully submit independent claims 1 and 8-11 are patentably distinct from the cited art, for at least the following reasons.

Independent claim 1 relates to a method of detecting a computer virus that attempts to gain access to restricted computer system resources, comprising, emulating computer executable code in a subject file, and monitoring the emulation of the computer executable code and monitoring a memory state of the computer system for modifications caused by the emulated instructions in the computer executable code, to detect an attempt by the emulated code to access one or more of the restricted computer system resources.

For example, according to embodiments of the present disclosure, the monitoring may include detecting installation of a new exception handler followed by forcing of a corresponding exception, detecting installation of a new interrupt handler followed by forcing of a corresponding interrupt, detecting writing of a new pointer to at least one predetermined address in system memory for storing an exception handler pointer, detecting writing of a new pointer to at least one predetermined address in system memory for storing an interrupt handler pointer, and detecting use of a predetermined instruction to retrieve an address in system memory corresponding to an interrupt descriptor table. Of course, the claims are not limited to the disclosed embodiments.

Nachenberg, as understood by the Applicant, relates to a polymorphic virus detection module that detects polymorphic viruses without emulating unnecessarily large numbers of instructions (Nachenberg, column 2, lines 48-50). For example, the emulation control module comprises virus profile data, a static exclusion module, and a dynamic exclusion module, which combine to substantially reduce the number of file instructions that must be emulated. (Nachenberg, column 6, lines 54-59). In other words, the emulation control module allows for the elimination of certain polymorphic viruses from consideration *prior* to emulation.

However, Applicant finds no teaching or suggestion in Nachenberg of a method of detecting a computer virus that attempts to gain access to restricted computer system resources, comprising, emulating computer executable code in a subject file, and monitoring the emulation of the computer executable code and monitoring a memory state of the computer system for modifications caused by the emulated instructions in the computer executable code, to detect an attempt by the emulated code to access one or more of the restricted computer system resources, as recited in independent claim 1.

Accordingly, the Applicant submits that independent claim 1 is patentably distinct from the cited art. Independent claims 8-11 are believed to be patentably distinct for at least similar reasons.

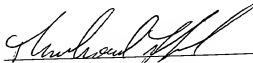
The Office is hereby authorized to charge any additional fees that may be required in connection with this amendment and to credit any overpayment to our Deposit Account No. 03-3125.

If a petition for an extension of time is required to make this response timely, this paper should be considered to be such a petition, and the Commissioner is authorized to charge the requisite fees to our Deposit Account No. 03-3125.

If a telephone interview could advance the prosecution of this application, the Examiner is respectfully requested to call the undersigned attorney.

Entry of this amendment and allowance of this application are respectfully requested.

Respectfully submitted,

A handwritten signature in dark ink, appearing to read 'Richard F. Jaworski', is written over a horizontal line.

RICHARD F. JAWORSKI

Reg. No.33,515

Attorney for Applicants

Cooper & Dunham LLP

Tel.: (212) 278-0400